Europäisches Patentamt	European Patent Office	Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.	The attached documents are exact copies of the European patent application described on the following page, as originally filed.	Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

01850012.4

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE, 28/02/01
LA HAYE, LE

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.: 01850012.4
Demande n°:

Anmeldetag:
Date of filing: 17/01/01
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
MICROSOFT CORPORATION
Redmond, Washington 98052-6399
UNITED STATES OF AMERICA

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Originator authentication

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE/TR
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

AWAPATENT AB
Kontor/Handläggare
Stockholm/Kenneth Ahrengart/KAT

MICROSOFT CORPORATION
Ansökningsnr
Vår referens
~~SE 2008998~~
EP 2018010

ORIGINATOR AUTHENTICATION

Technical Field

The present invention relates to methods, apparatuses and a system in connection with pushing of packet data from an originator to a wireless communication station.

Background of the Invention

Today, different kind of digital radio communications networks that support packet data transfer are being evolved. This means that mobile users having access to these radio communication networks are provided with the possibility to communicate packet data with different packet data networks, such as with the Internet, but also with corporate intranets and X.25 networks and the like. Thus, the digital radio, or wireless, communication network will be a wireless extension of, for example, the Internet and existing X.25 networks. Subscribers to such a radio communication network , i.e. the mobile users, will be able to benefit from most of the applications designed for these data packet protocols, such as Web browsing and exchange of e-mails etc., from their wireless equipment with which they access the wireless communication networks. Furthermore, a number of new mobile data services are currently being developed which will make use of these packet data transfer capabilities, while the performance of existing mobile data services will be improved.

Many of the new and existing mobile data services will make use of the possibility to push data to mobile users. Typically, to push data to a user means that a push server of a system or network automatically provides the user with some kind of information, i.e. the transfer of information is performed on the initiative of the push

server. Often this information is of the kind which is desired by the user, and therefore defined by a set of criteria in order to meet the desires of the user.

The technology of pushing information is today perhaps most widely used for pushing information to a stationary user, such as a user operating a computer connected to the Internet. However, with the rapid growth of mobile communications, in combination with the flexibility of being able to be reached by pushed information at any location, the possibility of receiving pushed information from a push server will become more and more interesting for users that are connected to wireless communication networks.

One of the most important grounds for the development described above is, besides the introduction of packet data transmissions to/from the wireless communication stations operated by the mobile users, the technology enhancements of the radio communications networks, such as the cellular radio communications networks, which provide higher and higher bandwidths for these packet data transmissions. Examples of wireless communication network with higher bandwidths and with support for packet data transfer to the wireless terminal of a mobile user are PDC-P networks (Pacific Digital Cellular), which in Japan provides the existing I-mode service, GSM networks (Global System for Mobile Communications) providing GPRS services (General Packet Radio Service), systems using radio networks based on EDGE technology (Enhanced Data Rates for GSM and TDMA/136 Evolution) or on WCDMA technology (Wideband Code Division Multiple Access), or any other forthcoming new generation of wireless communication networks which are known as UMTS networks (Universal Mobile Telephony Standard), or 3G networks, and which are based on the broadband radio networks WCDMA or cdma2000.

The pushing of packet data to a mobile user corresponds to a process in which the wireless

communication network initiates the packet data transfer to the user's wireless communication station, wherein the packet data being transferred most often is received by the wireless communication network from an external source, i.e. a push server on an external network which is operatively connected to the wireless communication network. When pushing information to a wireless communication station there are three important requirements that have to be met in order for a wireless communication network to be able to initiate the packet data transfer to the wireless station. These requirements are that 1) the wireless station has been switched on, 2) the wireless station has identified itself to those parts of the wireless communication network that provides the packet data service, and that 3) a Packet Data Protocol (PDP) address has been allocated to the wireless station.

After the requirements above have been met, measures are taken by the wireless network for initializing and activating a packet data service to the wireless station, measures that are well known in the art. After activation of the packet data service, packet data addressed to the PDP address that has been allocated to a wireless station will be routed to that station. A PDP address can be allocated to the station either as a static or a dynamic PDP address. Thus, the PDP address to be used by a server wishing to push data to a mobile communication station, i.e. to transfer data without the station having specifically requested the data, is either a permanent (static) or a temporary (dynamic) address allocated to that station.

The PDP address, irrespective of whether it is static or dynamic, needs to be known to a server that wishes to transfer packet data to the station. The PDP address can become known to the server by making an inquiry to the appropriate repository, possibly different repositories depending on whether static or dynamic

addresses are used, in the operator's wireless communication network.

In the Swedish patent application 9903637-8, filed on 8 October 2000, and incorporated herein by reference, a number of drawbacks related to the above described technique of inquiring for a mobile users PDP address are discussed. These drawbacks relate to the consequences of such things as: signaling load against the repository storing the PDP addresses; a change of the PDP address allocated to a specific mobile user from time to time; and the routing of PDP address requests to repositories.

The solution, according to the disclosure of the above identified patent application, is that a networks server, that wants to transfer packet data to a wireless communication station via a wireless communication network, requests that the wireless station sets up a Packet Data Protocol connection with the server. The request is accomplished by sending a message to the station, via a message service provided by the wireless network, using a subscriber's unique user identification number (such as a MSISDN number). In reply to the received message, which includes the packet data network address of the requesting server, the wireless station identifies itself to the packet data service part of the wireless network, if not already identified, activates a provided packet data service, if not already activated, and establishes a PDP connection with the requesting server. Using this PDP connection, the server may transfer packet data to the wireless communication station. This solution furthermore enables packet data to be transferred, or pushed, to a wireless station regardless of which current state the wireless station is in with respect to the packet data service of the wireless network.

When a packet switched connection, rather than a circuit switched connection, is used for transferring data to/from a user's wireless station, which for example

is the case when introducing GPRS in a GSM system, it will be possible for the mobile user to be constantly connected not only to the wireless network, but also to the Internet or some other packet data network via the wireless network and an interconnecting gateway. As the mobile user is constantly connected, the user will be charged for the actual bandwidth he uses. This means that the mobile user will be charged for each packet transmitted or received by the user, rather than for the time duration of the data transfer. Thus, a subscriber will be charged for any information received as packet data, regardless of which source that transfers, or pushes, the packet data to the subscriber.

The above described solution provided by the identified Swedish application 9903637-8 allows any network server to transfer a packet data network address to a subscriber by addressing the subscriber's unique user identification number. In this respect it would be desirable that the mobile user more easily could control to which network server he initiates a PDP connection. Moreover, it would be desirable that the mobile user could restrict the transfer of information to only be effectuated from a confined set of network servers. Furthermore, it would be desired to be able to take measures that prevents a network server outside of this confined set to transfer information to the user. A drawback with the Swedish patent application 9903637-8 is that the above described solution does not include any satisfactory means for restricting pushed information transfer to only be effectuated from certain desired network servers. Thus, it does not provide a secure manner for preventing that a mobile user receives non-desired information. Not only is reception of non-desired information time consuming and frustrating for the mobile user, it is also costly since the mobile user have to pay for the received packet data over his subscription bill from the operator.

The drawbacks described above regarding the reception of non-desired information from any network server, and the additional drawback of being charged by an operator for such information, are also present in any situation where a network server knows the packet data network address of the user in advance and uses this address for establishing a packet data session with the user's wireless station.

Summary of the Invention

An object of the present invention is to overcome at least one of the drawbacks described above that are present in connection with pushing packet data, i.e. transmission of packet data on an originator's own initiative, from an originator to a mobile user in a wireless communication network.

According to the present invention, said object is achieved by methods, a computer-readable medium, a wireless communication station and a system having the features as defined in the appended claims and representing different aspects of the invention.

According to the invention, the wireless communication station stores one or more predefined network addresses. When a network address is received by the wireless station from an originator wishing to push packet data to the wireless station, the received network address is checked against the stored predefined network addresses. If the received network address is found among the stored network addresses, the wireless station verifies the identity of the originator. The originator is determined to be authentic if the identity of the originator matches the possessor associated with the predefined network address. If the originator is authenticated, the wireless station establishes a packet data session with the originator. Using this packet data session, the originator may transfer, or push, packet data to the wireless station.

Thus, according to the invention, the wireless station has been pre-configured to only accept pushed packet data transmissions from one or more originators in possession of certain predefined network addresses. This means that the ability of network servers to push information to the wireless communication station is restricted to a certain confined set of one or more network servers. The identity verification combined with possessor information of a predefined network address(corresponding to the received network address), enables the wireless communication station to determine whether or not the originator in question indeed is the possessor of the received network address. Thus, it is ascertained that no information is received from a network server outside the confined set, not even if the originator has transmitted a "stolen" or "borrowed" network address to the wireless communication station.

Moreover, since the packet data session used for the information transfer from the network server is established by the wireless communication station, there is no need to beforehand provide any network server with the network address of the wireless communication station. An advantage with this, among others, is that a network server can not establish a session to the wireless communication station in order to transfer information, possibly non-desired, to the wireless station.

A further advantage provided by the establishment of the packet data session from the wireless station, is that the originator does not generate any signaling load against any repository in the wireless network storing packet data network addresses, something which otherwise can be a heavy burden on the repository when numerous originators, or servers, are trying to acquire packet network addresses to wireless stations connected to the wireless network. Furthermore, if dynamic packet data network addresses are used by the wireless network, which

most often is the case, the burden will be even heavier since the network address allocated to a specific wireless station will change from time to time. Moreover, when a wireless station is roaming between different wireless networks of different operators, the problem of determining to which operator's repository a server's requests for a packet data network addresses should be routed is avoided.

Preferably, the identity of an originator is verified by using an address translation server. Typically, an address translation server will upon request return the network server name corresponding to a certain network address. If someone has stolen a network address corresponding to a network address predefined by the wireless station, so called "spoofing", the address translation server will upon request indicate the true network server name that currently is associated with the network address. This is possible since an address translation server typically is designed to regularly check what network server name that corresponds to what network address, and to store these relationships in some kind of repository. The wireless station, or its user, will discover that the current originator does not correspond to the possessor of the predefined network address. Thus, the originator will be found not to be authentic and a packet data session will not be established with the originator.

Preferably, the wireless communication station determines that an originator, from which a network address is received, is authentic by comparing the network server name returned by the address translation server with a server name stored by the wireless communication station. The stored server name being stored by the wireless station in association with the stored network address that was found to match the received network address.

Advantageously, the network addresses stored and received by the wireless station are Internet Protocol (IP) addresses. In this case the address translation server is preferably a DNS server (Domain Name System) which upon reception of an IP address returns a server host name.

The establishment of a packet data session with the originating server is either made based on the network address, or, via the address translation server, based on the host name of the server. Preferably, an application executing in the wireless communication station, and controlling its operation, is responsible for the establishment of the packet data session. An originator is typically connected to a packet data network which is operatively connected to the wireless communication network. However, an originator may also be directly connected to the wireless communication network.

In an embodiment, use is made of an originator identification code. By verifying that a server, with which a packet data session is established for reception of packet data, uses the same identification code as the originator of a received network address, yet another security level is added.

The invention is also advantageous since the network addresses, from which the mobile user approves reception of packet data, are easily managed. A network address of an originator is quickly and easily added to, or deleted from, the storage space of the wireless communication station in which the network addresses are stored. Thus, the invention provides an immediate employment of added/deleted network addresses with respect to reception of packet data from the corresponding originators.

It is to be understood that what is meant by the expression wireless communication station in this document, sometimes herein referred to only as wireless station, is either a stand-alone RF (Radio Frequency) transceiver having processing capabilities and displaying

means, such as a mobile telephone or a hand-held PDA (Personal Digital Assistant), or, a RF transceiver together with any kind of portable or stationary equipment having processing capabilities, such as a portable laptop computer or a stationary personal computer, wherein the RF transceiver is arranged in communication with the portable or stationary equipment.

Even though the following description of an exemplifying embodiment will refer to a GSM network providing a GPRS service and an SMS-C (Short Message Service Center) providing a short message service, it is to be understood by those skilled in the art that the invention is not limited to these systems. The invention is advantageously applied to any wireless communication network that provides packet data transmissions to its connected users and that has an associated message service for transmitting short messages to the users. Such wireless communication networks have been exemplified in the background part of this application.

Brief Description of the Drawings

Further features and advantages of the invention will become more readily understood from the following detailed description of exemplifying embodiments of the invention when taken in conjunction with the accompanying drawings, in which:

Fig. 1 schematically shows an exemplifying overall system environment in which an embodiment of the invention is included and operable; and

Fig. 2 is a flow chart of an embodiment of a method according to the invention which is practiced by a wireless communication station.

Detailed Description of the Invention

With reference to Fig. 1, an exemplifying embodiment of the invention will know be described in greater detail. Fig. 1 shows a wireless communication network 10,

a wireless communication station 20, a node 30 for generating short messages for transmission to wireless communication stations, an address translation server 40, and an originator in the form of a network server 50 operatively connected to the wireless communication network 10. The wireless communication network is exemplified with a GSM network (Global System for Mobile Communication) and the wireless communication station with a GPRS mobile station. The packet data transferring capabilities of the GSM network 10 is provided by the GPRS service (General Packet Radio Service). GPRS being a standardization from the European Telecommunications Standard Institute (ETSI) on packet data in GSM systems. The node for generating short messages is exemplified with a SMS-C (Short Message Service Center) and the address translation server with a DNS server (Domain Name System). The network server 50 could be any server connected to the Internet or to a corporate Intranet to which the wireless communication network 10 is operatively connected by means of an appropriate gateway (not shown).

The architecture and operation of a GSM Network providing a GPRS service, as well as the standardization thereof, should be well known to persons skilled in the art. For this reason, only those features or aspects of GSM and GPRS that are of direct relevance to this described embodiment of the invention will be described herein.

A GSM network 10 which includes a GPRS service for handling packet data traffic is equipped with a Serving GPRS Support Node (SGSN) (not shown) and a Gateway GPRS Support Node (GGSN) (not shown). The SGSN is the node within the GSM infrastructure that sends and receives packet data to and from a wireless GPRS mobile station 20 via a Base Station System (not shown). The GPRS mobile station 20 communicates with the Base Station System over an air interface in accordance with the standardization

of GSM and GPRS. The SGSN also transfers packets between the GPRS station 20 and the GGSN. Furthermore, the SGSN handles PDP contexts (Packet Data Protocol) for connections with any server in any external packet data network, such as with the network server 50 which is operatively connected to the GSM network 10. The GGSN, which is connected to the SGSN, is the gateway of the GSM/GPRS system to external packet data networks and routes packets between the SGSN and an external packet data network, e.g. the Internet or an corporate Intranet. For more information about GPRS, reference is made to ETSI standardization documents EN 301 113 V6.1.1 (1998-11) and Draft ETSI EN 301 344 V6.4.0 (1999-08), both documents which are incorporated herein by reference.

Furthermore, the architecture and operation of the SMS-C and the DNS server are well known to persons with ordinary skills in the art, thus, only features of direct relevance to the present embodiment will be described herein.

The wireless communication station of the present invention, i.e. the GPRS mobile station 20 in the embodiment of Fig. 1, includes a state of the art microprocessor 21, a main memory 22 implemented by read only memory (ROM) and/or random access memory (RAM) or equivalents thereof, Input/output circuitry (not shown), such as a display and a keyboard/keypad, for communicating with a user, interface circuitry 23 in the form of transmitting/receiving radio frequency circuitry for communicating with the GSM network via an antenna 25 and the air interface, a bus 24 interconnecting the elements of the GPRS mobile station, as well as other appropriate components. Of these elements, at least some are controlled or otherwise designed to facilitate the practice of the method of the invention.

The microprocessor 21 executes appropriate computer-executable components stored in the main memory 22, thus controlling the elements and the overall wireless

communication station/GPRS mobile station 20 to function in accordance with the method of the invention. Alternatively, these computer-executable components are stored on a pre-recorded disk, in a pre-programmed memory device, or any other computer-readable medium being separate from the wireless communication station 20. When the wireless communication station 20 and its included microprocessor 21 is provided with access to this computer-readable medium, its stored computer-executable components will direct the microprocessor 21 to control the overall wireless communication station 20 to function in accordance with the method of the invention.

The operation of the wireless communication station/GPRS mobile station 20 will be more fully understood from the description below and from the description of the flow chart shown in Fig. 2.

The operation of the overall system and of the wireless communication station/GPRS mobile station in Fig. 1 in accordance with the embodiment will now be described in a step by step fashion, wherein each step has a reference numeral in Fig. 1. The described operation is started when the originator, i.e. the network server or push server 50, wants to push packet data over a TCP/IP connection to a GPRS subscriber operating a GPRS mobile station 20.

1. In step 1 the push server 50 connects to the SMS-C 30 and submits a request that an SMS message (Short Message Service) should be generated and transmitted to a GPRS subscriber having a particular MSISDN number (Mobile Station Integrated Services Digital Network) in accordance with the numbering plan used. This is performed over a transport protocol, such as TCP/IP or X25, in accordance with techniques that are well known to persons skilled in the art. The push server includes its own network address, i.e. its Internet Protocol (IP) address if the push server is connected to the Internet

or an Intranet, in the submitted request. Furthermore, the push server 50 generates an identification code which is included in the submitted request as an originator identification code. A port number to be used when setting up a TCP/IP-based connection towards the server 50 is included in the request.

2. In step 2 the SMS-C 30 transmits the generated SMS message with the push server's 50 IP address and its generated originator identification code to the GPRS mobile station 20. The transmission is performed through the GSM/GPRS network 10 over a GSM signaling channel or on a GPRS traffic channel in accordance with state of the art techniques.

3. In step 3, an application already executing in the GPRS mobile station 20, or, which is started when the SMS message is received, extracts the payload of the SMS message. The SMS message could e.g. include an activation code, and if this code corresponds to a predefined code which is accepted by the application, the application processing proceeds, otherwise the application processing is stopped. Thus, if no activation code is found, the SMS message is treated in the usual way, which is outside the scope of the present invention. If the activation code is present, the application extracts the payload of the SMS message, i.e. the received IP address, port number and originator identification code. The application then checks the IP address received in the SMS message against a set of stored IP addresses. These stored IP addresses has previously been defined by the subscriber and are stored in a memory accessible to the application, either in an internal RAM memory 22 of the GPRS station 20 or in an external memory, such as on a SIM (Subscriber Identity Module) card (not shown) connected to the GPRS station

20. The stored IP addresses, or the stored IP address, corresponds to those, or the, push server(s) from which the GPRS subscriber wants to be able to receive pushed packet data.

If a match is found by the GPRS station 20 among the stored IP addresses, the received originator identification code is saved and a TCP/IP connection is set up towards the DNS server 40. This TCP/IP connection is preferably set up in accordance with the GPRS connection phase described below. The IP address received in the payload of the SMS message is then sent to the DNS server 40 over the established TCP/IP connection.

4. In step 4 the DNS server 40 looks up the IP address to find the corresponding server host name. When found, the matching server host name is transmitted back to the GPRS station 20 over the TCP/IP connection. Thus, the GPRS station 20 is provided with the host name of the server 50 wishing to push information to it.

5. In step 5 the GPRS station 20 now authenticates the push server 50, i.e. it checks if the push server is the actual possessor of the received IP address. This is performed by examining the resulting host name returned from the DNS server 40 with respect to the server host names stored in association with the predefined IP addresses that are stored by the GPRS station 20. The application checks the received server host name by comparing it with the server host name that is stored in association with the predefined IP address that was found to match the earlier received IP address. Alternatively, the application of the GPRS station 20 displays the host name received from the DNS server 40 to the mobile user on a display of the GPRS station 20, after which the mobile user, if the host name is recognized, manually (e.g. by pressing a key on a keypad) verifies that the returned host name corresponds to one of the stored

predefined IP addresses. If the push server was determined to be authentic, i.e. if it was determined to be the true possessor of the received IP address, the application processing continues to the GPRS connection phase.

As previously described in the background section, when pushing information to a wireless communication station, there are three requirements that have to be met in order for a wireless communication network to be able to initiate the packet data transfer to the wireless station. These requirements, which are part of the GPRS connection phase, include that 1) the wireless station has been switched on, 2) the wireless station has identified itself to those parts of the wireless communication network that provides the packet data service, and that 3) a Packet Data Protocol (PDP) address has been allocated to the wireless station.

In a GSM/GPRS network 10, after the requirements above have been met, measures are taken by the GSM/GPRS network for initializing and activating a packet data service to the wireless GPRS station 20, measures of the GPRS connection phase that are well known in the art. After activation of the packet data service, packet data addressed to the PDP address that has been allocated to a GPRS station 20 will be routed to that station. As described in the background section, the PDP address allocated to the GPRS station 20 is either a permanent (static) or a temporary (dynamic) address allocated to that station.

Thus, in the GPRS connection phase the application identifies the GPRS station 20 for the packet data service part of the GSM/GPRS network 10, if it is not already identified. This corresponds to checking whether the GPRS station 20 is GPRS attached or not. If the GPRS station is not attached, the application performs a GPRS attach. The GPRS attach is preferably performed in accordance with standard procedure, see for example Draft

ETSI EN 301 344 V6.4.0 (1999-08), chapter 6.2. The GPRS application then checks if the GPRS station 20 has a valid IP-address(i.e. if it has a working TCP/IP connection). If not, the application requests the GSM/GPRS network 10 to activate a packet data service to be used by the GPRS station 20, i.e. it initiates the performance of a GPRS PDP Context Activation. The GPRS application then either receives a dynamically allocated IP-address from the GSM/GPRS network 10 or from a Radius server (not shown) via the GSM/GPRS network. The GPRS PDP Context Activation and the transfer of a dynamic IP-address are preferably performed in accordance with standard procedure, see for example TS 101 348 V6.3.0 (1998-10), chapter 11.2.1.2. Of course, the GPRS application could alternatively already have a static IP address allocated to it when initiating the GPRS PDP Context Activation.

The application of the GPRS station 20 then initiates establishment of a TCP/IP connection towards the IP-address and the port number received in the SMS message. The IP address and the port number designates the server 50 and a server application wishing to push packet data. Alternatively, when establishing the connection, the push server 50 is identified using the server host name received from the DNS server 40.

6. In step 6 the push server 50 recognizes that a TCP/IP connection has been set up from the GPRS station 20 to which it earlier initiated the transmission of an SMS message in order to accomplish the now established connection. This recognition is based on information which the GPRS station 20 has included in the response message, e.g. the MSISDN of the GPRS station 20 or a request code originally generated and included in the SMS message previously transmitted by the server 50. The push server 50 responds by first transmitting the same

originator identification code which it earlier transmitted in the SMS message to the GPRS station. This will enable the GPRS station to verify that the push server 50 to which a TCP/IP connection now is established is the same server as that which transmitted the original SMS message triggering the set-up of the connection. After transmission of the identification code the push server 50 starts transmitting packet data with information to the GPRS station 20.

In Fig. 2 a flow chart of the operation of a wireless communication station/GPRS mobile station and its included executing application is shown.

In step S1 the mobile user enters the IP address(es), and preferably the corresponding server host name(s), of the server(s) 50 from which it is desired to receive pushed packet data. The IP addresses and corresponding host names, as well as the address of the DNS server 40, are stored in a memory 22 of the GPRS station 20 for later retrieval by an application executing in the GPRS station. Alternatively, this step S1 relates to the actual loading of an application in the GPRS mobile station, which application already includes the IP addresses and corresponding host names of predefined originators from which the GPRS station shall be able to receive pushed packet data.

In step S2 the application of the GPRS station receives an SMS message from which payload it extracts an IP address, a port number and an originator identification code. The application then in step S3 checks whether or not the received IP address matches any of the stored IP addresses. If no match is found, the application execution returns to step S2. If a match is found, the execution continues to step S4, in which step the received originator identification code is stored.

In step S5 the application establishes a TCP/IP connection with the DNS server using the pre-stored IP address. It then in step S6 transmits the IP address received in the SMS message and requests the DNS server to perform an address translation. In response to the request, the application in step S7 receives a host name from the DNS server. In step S8 the received host name is checked for a match against the host name stored in association with the stored IP address that corresponded to the IP address received in the SMS message. If no match is found, the originator is determined not to be authentic and the execution returns to step S2. If a match is found the execution continues to step S9.

In step S9 the application establishes a TCP/IP connection with the originator of the IP address received in the SMS message, i.e. with the push server 50. It then once again receives an originator identification code from the push server, this time in step S10 over the TCP/IP connection, which code in step S11 is matched against the identification code previously received in the SMS message. If no match is found, the execution returns to step S2. If a match is found, the execution continues to step S12 in which packet data transmissions are accepted and received from the push server.

Although the invention has been described with reference to a specific exemplifying embodiment based on a GSM system providing a GPRS service, many different alterations, modifications and the like will become apparent for those skilled in the art. The described embodiments are therefore not intended to limit the scope of the invention, as defined by the appended claims. Instead, it is to be understood that the present invention is well suited for any wireless communication network that provides a packet data service to its connected wireless users.

CLAIMS

1. A method at a wireless communication station, the station being operatively associated with a wireless communication network providing packet data transferring services, the method including the steps of:

receiving a network address of an originator of packet data;

verifying the identity of the originator, if the received network address matches a predefined network address included in a set of one or more predefined network addresses stored by the wireless communication station; and

establishing, if the originator is authentic, a packet data session with the originator in order to facilitate transfer of packet data from the originator,

thereby ascertaining that pushed packet data only is received from one or more predefined originators.

2. The method as claimed in claim 1, wherein each of said predefined network addresses of said set is associated, within the wireless communication station, with a name of a network server from which it is desired to receive packet data.

3. The method as claimed in claim 1 or 2, wherein said verifying step includes:

establishing a packet data session with an address translation server;

requesting translation of the network address to a corresponding name of a network server; and

determining, based upon the result of said translation, whether or not the network address is authentic.

4. The method as claimed in claim 3, wherein said determining step includes comparing the network server name returned by said address translation server with a

previously stored network server name, the stored name being stored by the wireless communication station in such way that it is associated with the predefined network address matching said received network address.

5. The method as claimed in any one of claims 1 - 4, wherein said network address of said receiving step is received in a short message, the short message being received from a short message service provided by said wireless communication network.

6. The method as claimed in any one of claims 1 - 5, wherein said step of establishing a packet data session with the originator includes establishing a packet data session using the network address of said receiving step.

7. The method as claimed in any one of claims 1 - 6, wherein said network address is an Internet Protocol address.

8. The method as claimed in any one of claims 3 - 5, wherein said step of establishing a packet data session with the originator includes establishing a packet data session using the name of the network server, which name is returned by the translation server.

9. The method as claimed in any one of claims 3 - 8, wherein said name of the network server is an Internet domain host name of the network server.

10. The method as claimed in any one of claims 1 - 9, further including:

receiving a first originator identification code in said receiving step;

receiving a second originator identification code over the packet data session established with the originator; and

verifying, based on a comparison between the first and the second identification code, that the packet data session was established with the originator of the received network address.

11. A computer-readable medium storing computer-executable components for causing a wireless communication station to perform the steps recited in any one of claims 1 - 10 when the computer-executable components are run on microprocessor included by a wireless communication station.

12. A wireless communication station arranged to be operatively associated with a wireless communication network providing packet data transferring services, wherein the wireless communication station includes processing means, memory means and interface circuitry means for performing the steps recited in any one of claims 1 - 10, thereby ascertaining that pushed packet data only is received from one or more predefined originators.

13. A method of a system which includes a wireless communication station and an originator of information, the station being operatively associated with a wireless communication network providing packet data transferring services, the method including the steps of:

transmitting, from the originator to the wireless communication station, the originator's own network address;

verifying, at the wireless communication station, the identity of the originator, if the received network address matches a predefined network address included in a set of one or more predefined network addresses stored by the wireless communication station;

establishing, from the wireless communication station, and if the originator is determined by the

wireless communication station to be authentic, a packet data session with the originator in order to facilitate transfer of packet data from the originator,

thereby ascertaining that pushed packet data only is received from one or more predefined originators.

14. The method as claimed in claim 13, wherein each of the predefined network addresses of said set is associated, within the wireless communication station, with a name of a network server from which transfer of packet data to the wireless communication station is desired.

15. The method as claimed in claim 13 or 14, wherein said verifying step includes:

establishing, from the wireless communication station, a packet data session with an address translation server;

requesting, from the wireless communication station, translation of the network address to a corresponding name of a network server; and

determining, at the wireless communication station, and based upon the result of said translation, whether or not the network address is authentic.

16. The method as claimed in claim 15, wherein said determining step includes comparing, at the wireless communication station, the network server name returned by said address translation server with a previously stored network server name, the stored name being stored by the wireless communication station in such way that it is associated with the predefined network address matching said received network address.

17. The method as claimed in any one of claims 13 - 16, wherein said network address of said transmitting

step is transmitted by requesting a short message service provided by a wireless communication network to transmit a short message that includes said network address to the wireless communication station.

18. The method as claimed in any one of claims 13 - 17, wherein said step of establishing a packet data session with the originator includes establishing, from the wireless communication station, a packet data session using the network address received as a result from said transmitting step.

19. The method as claimed in any one of claims 13 - 18, wherein said network address is an Internet Protocol address.

20. The method as claimed in any one of claims 15 - 17, wherein said step of establishing a packet data session with the originator includes establishing, from the wireless communication station, a packet data session using the name of the network server, which name is returned by the translation server in said verifying step.

21. The method as claimed in any one of claims 15 - 20, wherein said name of the network server is an Internet domain host name of the network server.

22. The method as claimed in any one of claims 13 - 21, further including:

transmitting a first originator identification code in said transmitting step;

transmitting, from the originator, a second originator identification code over the packet data session established between the wireless communication station and the originator; and

verifying, at the wireless communication station, and based on a comparison between the first and the second identification code, that the packet data session was established with the originator of the network address received in said transmitting step.

23. A system including a wireless communication station and at least one originator server, the station being operatively associated with a wireless communication network providing packet data transferring services, wherein the system is arranged to perform the steps recited in any one of claims 13 - 22, thereby ascertaining that the wireless communication station only receives pushed packet data from one or more predefined originators.

Abstract of the Invention

The present invention relates to methods, apparatuses and a system in connection with pushing of packet data from an originator to a wireless communication station 20. When a network address is received by the wireless station 20 from a server 50 wishing to push packet data to the wireless station, the received network address is checked against stored predefined network addresses. If the received network address is found among the stored network addresses, the originator is verified, preferably by using an address translation server 40. Thus, in this way it can be determined that the originator indeed belongs to a predefined set of originators from which a mobile user wants to accept pushed packet data transmissions. A packet data session is then established by the wireless station with a verified originator in order to receive the packet data.

Fig. 1

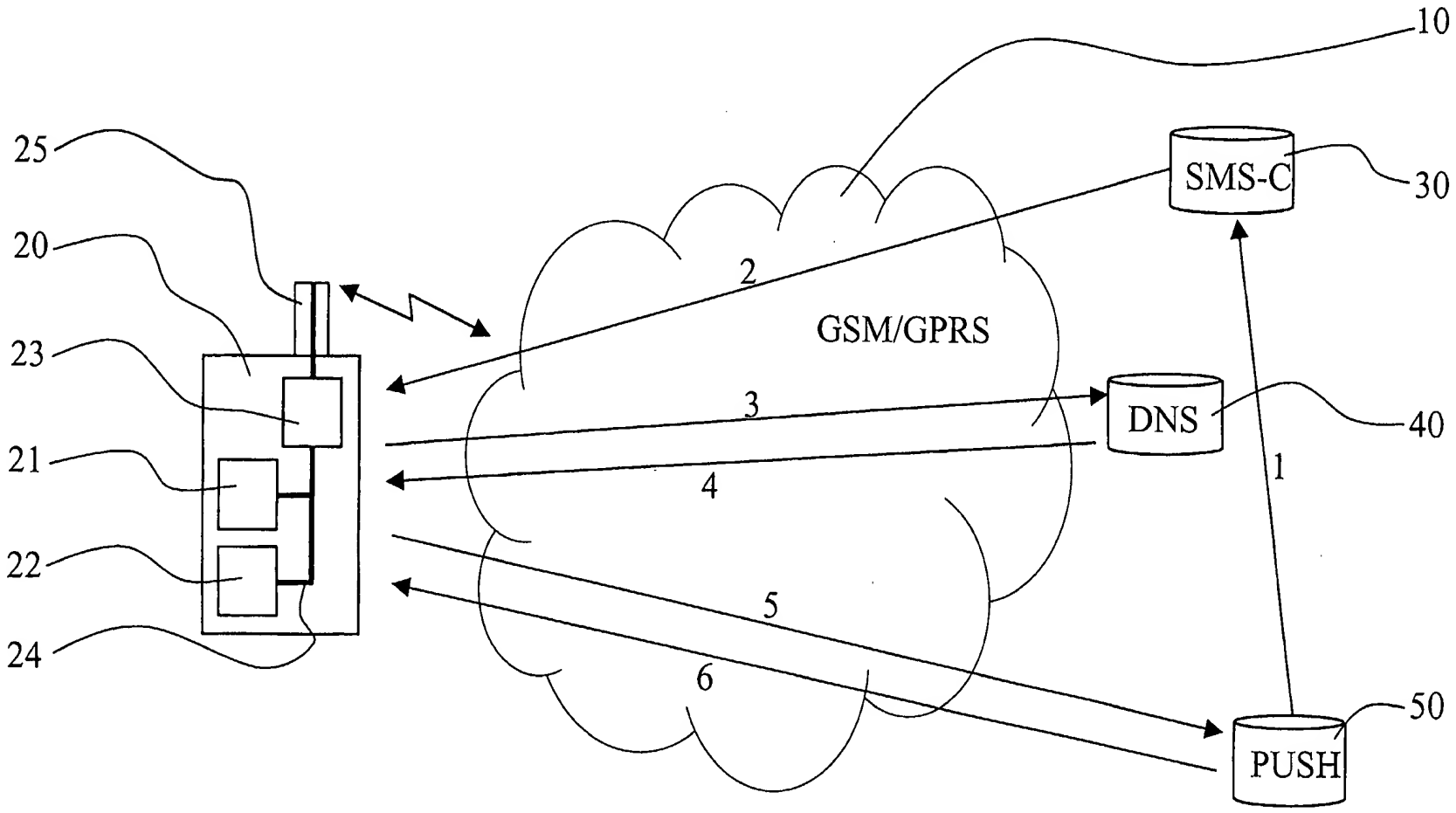

FIG. 1

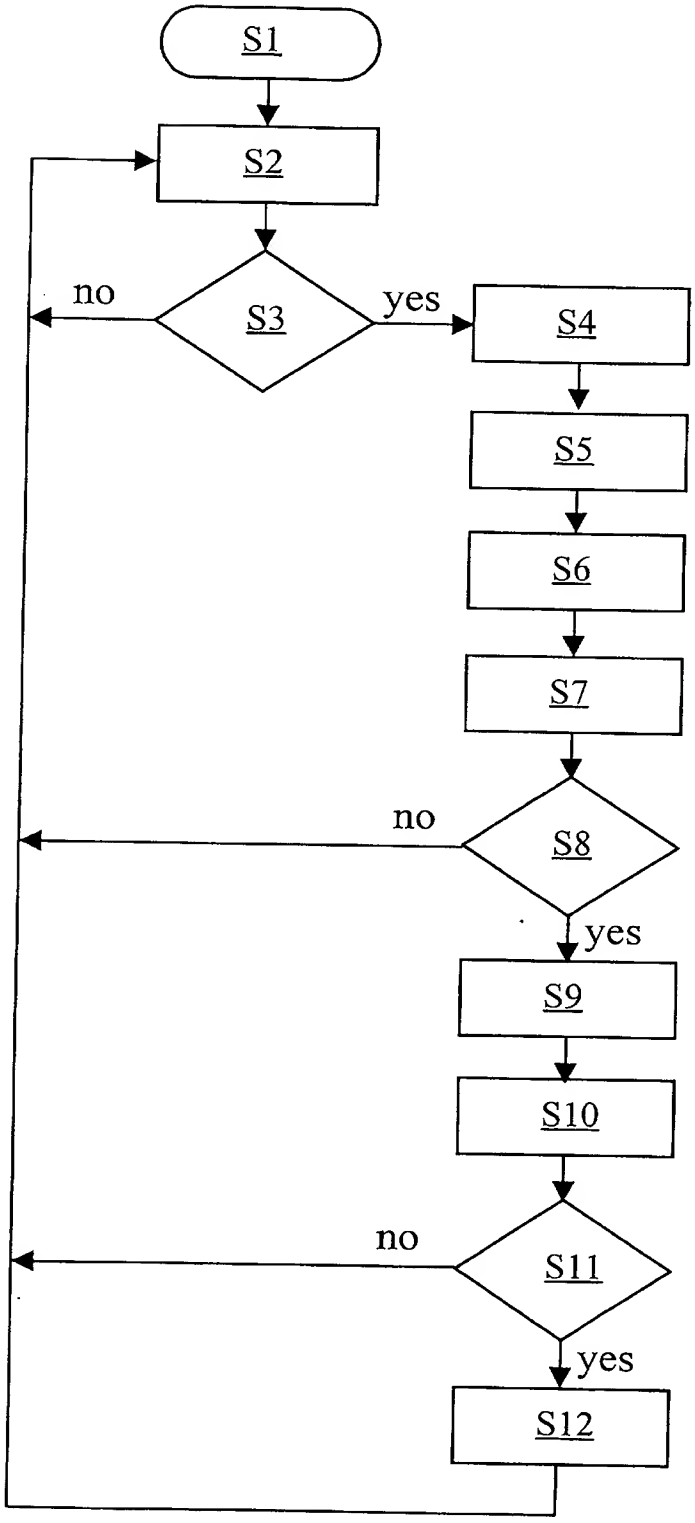

FIG. 2